Anwenderforum für Fernmeldetechnik, AFCEA Computer, Elektronik und Automatisierung

AFCEA Bonn e.V. Studienpreis 2017

Kernthesen der Arbeit

Titel der Arbeit:	Intelligence-Driven Alert Generation For Intrusion Detection
Tag der Einreichung:	23.01.2017
Hochschule:	Rheinische Friedrich-Wilhelms-Universität Bonn
Name des Verfassers:	Marc-Philipp Ohm
Betreuender Professor:	Prof. Dr. Michael Meier

*Kurze Beschreibung (1 Seite !) der **Kernthesen**.*

Was ist die Quintessenz der Arbeit?

Der Begriff der Threat Intelligence bezeichnet Informationen über Bedrohungen. Herkömmlicherweise wird Threat Intelligence in einem Szenario verwandt, in dem eine Partei Informationen über eine Bedrohung sammelt und diese anschließend einer oder mehreren anderen Parteien zur Verfügung stellt, sodass sich diese auf die beschriebene Bedrohung vorbereiten können.

Der in dieser Arbeit vorgestellte Ansatz ermöglicht die Vereinigung dieser Teilprozesse, nämlich der vollständigen Automatisierung der Erzeugung sowie des Konsums von Threat Intelligence, sodass es möglich wird, den Prozess als Ganzen zu betrachten. Unter Zuhilfenahme von dynamischer Analyse von Schadsoftwareexemplaren werden Threat Intelligence Berichte im weitverbreiteten STIX Format erzeugt. Schadsoftware stellt lediglich eine mögliche Art von Bedrohung dar, ist jedoch gut observierbar und erzeugt nachvollziehbare Spuren auf einem Hostsystem beziehungsweise in einem Netzwerk durch Persistenzmechanismen oder Command and Control Netzwerkverkehr. Zusätzlich ist diese Form der Bedrohung reproduzierbar, sodass gewonnenen Informationen als Indikatoren zur Erkennung eingesetzt werden können.

Um eine Erkennung sowohl auf dem Hostsystem als auch im Netzwerk zu ermöglichen, wurden zwei bereits entwickelte Teillösungen verwandt. Diese sind in der Lage die im STIX Bericht enthaltenen Informationen in die programmspezifische Syntax der Sicherheitsprogramme GRR Rapid Response sowie Suricata zu überführen. GRR löst dabei das Teilproblem der host-basierten Erkennung der von durch Schadsoftware verursachter Spuren. Ergänzend analysiert Suricata, als Teil seiner Aufgabe als Network Intrusion Detection System, den mitgeschnittenen Netzwerkverkehr auf beobachtbare Spuren.

Durch die Automatisierung des Prozesses von der Schadsoftwareanalyse über den Austausch von Informationen bis hin zur Wiedererkennung der Schadsoftware, konnten im Rahmen der Arbeit rund 3000 Schadsoftwareexemplare bearbeitet werden. Die daraus gewonnen Erkenntnisse wurden verwandt, um die Erkennungs- sowie die Klassifikationsrate zu verbessern.

Es war zu beobachten, dass alle Berichte durch ohnehin auf dem Hostsystem oder im Netzwerk befindliche Spuren „verunreinigt“ waren, sodass diese aus den endgültigen Berichten entfernt werden mussten, um Fehlalarme zu vermeiden. Die entstandenen „bereinigten“ Berichte wiesen eine hohe Spezifität bei gleichzeitig hoher durchschnittlicher Anzahl an Indikatoren auf. Im Gegensatz dazu wurden während der erneuten Ausführung der Schadsoftwareexemplare vergleichsweise wenige Indikatoren wiedergefunden, wodurch die präzise Alarmgenerierung erschwert wird.

Für die Aufgabe der Alarmgenerierung wurden einerseits der Standardansatz, nämlich das Vorhandensein aller Indikatoren, geprüft und andererseits zwei schwellwertbasierte Verfahren ausgewertet. Dabei konnte gezeigt werden, dass der Standardansatz unzureichend ist, wohingegen die neu vorgestellten Ansätze eine bedeutend bessere Erkennungs- sowie Klassifikationsrate erzielen. Des Weiteren konnte durch eine Gewichtung der Indikatoren eine weitere Verbesserung der Spezifität der Alarme erwirkt werden.